Subject: Ensuring Compatibility with SHA-2 and FIPS 140-3 Compliant Cryptographic Devices

All Software Developers, Application Service Providers, Web Portal Owners, System Integrators, Government Departments, Certifying Authorities (CAs), and other entities using Digital Signature Certificates (DSCs) shall ensure that their applications and services support SHA-2 based cryptographic operations, in accordance with the Guidelines and specifications issued by the Controller of Certifying Authorities (CCA).

The CCA Interoperability Guidelines mandate SHA-256 based signature algorithms, including SHA256 with RSA and ECDSA with SHA256. The eSign API specifications also mandate SHA-256 for document hashes and signature hash algorithms.

Accordingly, applications, APIs, middleware, signing components and backend services used for DSC-based operations shall use SHA-2 based algorithms and shall not use deprecated hash algorithms such as SHA-1 and MD5 for generation of new digital signatures, document hashes or timestamps.

Stakeholders shall review and update their applications, cryptographic libraries, middleware, PKCS#11 modules, CSP/KSP etc. implementations and related interfaces to remove dependencies on deprecated algorithms and ensure compatibility with SHA-2 and FIPS 140-3 compliant cryptographic tokens/HSMs.

All audit agencies shall verify compliance with the above requirements. Any use of, or dependency on, SHA-1, MD5 or other deprecated hash algorithms for generation of new digital signatures, hashes or timestamps shall be reported to the auditee for appropriate corrective action and O/o CCA at info@cca.gov.in immediately.

All concerned organizations are advised to complete the required software modifications and testing well in advance w.r.t the timelines stipulated in CCA's Advisory Note on FIPS 140-2 to FIPS 140-3 Migration (available at: https://cca.gov.in/sites/files/pdf/news/Advisory_on_Migration_from_FIPS_140-2_to_FIPS_140-3.pdf) to ensure seamless interoperability with FIPS 140-3 compliant cryptographic devices and continued availability of Digital Signature services.

This is issued in the public interest to strengthen the security posture of India's Public Key Infrastructure (PKI), Digital public trust ecosystem and enhance the security, integrity, interoperability and trustworthiness of digital transactions.

Office of the Controller of Certifying Authorities
Ministry of Electronics and Information Technology
Government of India